In the Claims

1. (Currently amended) A computerized method for restricting network access by applications comprising:

detecting a network access request from an application;

examining an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network; and

blocking access to the network if the application is not authorized to access the network.

2. (Original) The method of claim 1 further comprising:

determining a network resource requested by the application;

examining the application policy file to determine if the application is authorized to access the network resource; and

allowing access to the network resource if the application is authorized to access the network resource.

3. (Original) The method of claim 1 further comprising:

determining a type of network access requested by the application;

examining the application policy file to determine if the application is authorized for the type of network access requested; and

allowing the type of network access requested if the application is authorized for the type of network access requested.

4. (Original) The method of claim 1 further comprising:

updating the application policy file; and

re-evaluating applications currently executing against the updated policy file.

5. (Currently amended) The method of claim 1, ~~further comprising:~~

~~determining if the application is allowed access to the network based on an~~ wherein the application identifier is in the network access request.

6. (Original) The method of claim 1, wherein the method is performed on a client computer on which the application is executing.

7. (Currently amended) A computer-readable medium having executable instruction to cause a computer to perform a method comprising:

detecting a network access request from an application;

examining an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network; and

blocking access to the network if the application is not authorized to access the network.

8. (Original) The computer-readable medium of claim 7, wherein the method further comprises:

determining a network resource requested by the application;

examining the application policy file to determine if the application is authorized to access the network resource; and

allowing access to the network resource if the application is authorized to access the network resource.

9. (Original) The computer-readable medium of claim 7, wherein the method further comprises:

determining a type of network access requested by the application;

examining the application policy file to determine if the application is authorized for the type of network access requested; and

allowing the type of network access requested if the application is authorized for the type of network access requested.

10. (Original) The computer-readable medium of claim 7, wherein the method further comprises:

updating the application policy file; and

re-evaluating applications currently executing against the updated policy file.

11. (Currently amended) The computer-readable medium of claim 7, wherein the ~~method further comprises:~~

~~determining if the application is allowed access to the network based on an~~ application identifier is in the network access request.

12. (Currently amended) A computer system comprising:

a processing unit;

a memory coupled to the processing unit through a bus;

a network interface coupled to the processing unit through the bus and further operable for coupling to a network; and

an application policy process executed from the memory by the processing unit to cause the processing unit to detect a network access request from an application, to examine an application policy file to determine if the application is authorized to access the network by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, and to block access to the network if the application is not authorized to access the network.

13. (Original) The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a network resource requested by the application, to examine the application policy file to determine if the application is authorized to access the network resource, and to allow access to the network resource if the application is authorized to access the network resource.

14. (Original) The computer system of claim 12, wherein the application policy process further causes the processing unit to determine a type of network access requested by the application, to examine the application policy file to determine if the application is authorized for the type of network access requested, and to allow the type of network access requested if the application is authorized for the type of network access requested.

15. (Original) The computer system of claim 12, wherein the application policy process further causes the processing unit to update the application policy file, and to re-evaluate applications currently executing against the updated policy file.

16. (Currently amended) The computer system of claim 12, wherein the ~~application policy process further causes the processing unit to determine if the application is allowed access to the network based on an~~ application identifier is in the network access request.

17. (Original) The computer system of claim 12, wherein the application is executed from the memory by the processing unit.

18. (Currently amended) A computer-readable medium having stored thereon an application policy data structure comprising:

an application identifier field containing data identifying an application that is authorized for installation on computer coupled to a network;

a network identifier field containing data identifying a entity that is accessible by the application identified by the application identifier field; and

an access flag field containing data specifying whether the application identified by the application identifier field is allowed access to the entity identified by the network identifier field.

19. (Original) The computer-readable medium of claim 18 further comprising:

an additional policy rule field containing data specifying whether the application identified by the application identifier field is allowed a particular type of access to the entity identified by the network identifier field.

20. (Original) The computer-readable medium of claim 18 further comprising:

a response field containing data specifying an action to performed if the application identified by the application identifier field attempts access to the entity identified by the network identifier field and the access is not allowed.

21. (Original) The computer-readable medium of claim 18, wherein the entity is selected from the group consisting of a network and a network resource.

22. (New) The method of claim 5, wherein the application identifier is selected from the group consisting of a file name of the application and a path on the network.

23. (New) The method of claim 5, wherein a plurality of the application identifiers are associated with each application, and each of the application identifiers corresponds to a different network address assigned to the corresponding application.

24. (New) The method of claim 1, wherein each application entry in the application policy file comprises a set of access policy rules for one of a network and a network resource identified by a network identifier.

25. (New) The method of claim 24, wherein the network identifier is selected from the group consisting of a network address range and a Universal Naming Convention path.

26. (New) The method of claim 24, wherein the set of access policy rules includes a first rule that allows DNS service from a specified network server, and a second rule that disallows FTP with respect to specified addresses.

27. (New) The method of claim 26, wherein a null setting for an access flag is interpreted as one of allowing and disallowing all access to a network specified by the network identifier.

28. (New) The method of claim 1 wherein the application policy file includes an application identifier, a network identifier, an access flag, additional policy rules, and at least one application entry.

29. (New) A computerized method for execution on a computer coupled to a network to restrict network access by an application executing on the computer, the method comprising:

detecting a network request from the application, the request comprising at least one of an identifier and entity and a type of network access, wherein the entity is one of a network and a network resource;

examining an application policy file to determine if the application is authorized to access the entity by comparing an identifier for the application with identifiers in the application policy file that correspond to applications authorized for installation on computers coupled to the network, wherein each application entry in the application policy file comprises a set of access policy rules for a network corresponding to a network identifier, the network identifier comprising at least one of a network address range and a Universal Naming Convention path, and wherein the application policy file further comprises an access flag having a null setting that is interpreted as one of allowing and disallowing all access to a network specified by the network identifier;

blocking access to the entity if the application is not authorized to access the entity; and

re-evaluating applications currently executing against any updated application policy file,

wherein a plurality of the application identifiers are associated with each application, each application identifier corresponding to a different network address assigned to the corresponding application, and wherein each application identifier is one of a file name of the application and a path on the network.